Amendments to the Claims

1. (previously presented) A method of generating encrypted packets comprising the steps of:

receiving in a security processor a first Ethernet packet comprising a second Ethernet packet and a memory address associated with a security association;

extracting the memory address and the second Ethernet packet from the first Ethernet packet;

retrieving the security association from the memory using the received memory address; and

encrypting a portion of the extracted second Ethernet packet according to the retrieved security association.

2. (previously presented) The method of claim 1 wherein the first Ethernet packet also includes outer Ethernet header and a manufacturer header.

3. (previously presented) The method of claim 2 wherein the manufacturer header includes the memory address.

4. (previously presented) The method of claim 3 wherein the outer Ethernet header comprises an Ethernet address of the security processor.

5. (previously presented) The method of claim 4 wherein the outer Ethernet header comprises a user-specific type field.

6. (previously presented) The method of claim 5 wherein a first byte of the manufacturer header is set to zero.

7. (currently amended) The method of claim 6 wherein a portion of the manufacturer header following the first byte of the manufacturer header ~~the second, third and fourth bytes~~ includes the memory address.

8. (canceled)

9. (previously presented) The method of claim 1 wherein the extracting step comprises determining whether an Ethernet type field from the first Ethernet packet comprises a user-specific Ethernet type.

10-12. (canceled)

13. (previously presented) The method of claim 1 wherein the retrieving step comprises retrieving the at least one security association from a memory in the security processor.

14. (previously presented) The method of claim 1 wherein the encrypting step comprises using an encryption key associated with the security association.

15. (previously presented) The method of claim 1 wherein the encrypting step comprises using an encryption algorithm defined by the security association.

16. (previously presented) The method of claim 1 wherein the extracting step comprises determining whether an Ethernet address from the first Ethernet packet matches an Ethernet address of the security processor.

17. (previously presented) A method of generating encrypted packets by processing a first Ethernet packet comprising a second Ethernet packet and a memory address associated with a security association, the method comprising the steps of:

extracting the memory address and the second Ethernet packet from the first Ethernet packet;

retrieving the security association from the memory using the extracted memory address; and

encrypting a portion of the extracted second Ethernet packet according to the retrieved security association.

18. (previously presented) The method of claim 17 wherein the extracting step comprises determining whether an Ethernet type field from the first Ethernet packet comprises a user-specific Ethernet type.

19. (previously presented) The method of claim 17 wherein the extracting step comprises determining whether a first byte following an Ethernet type field from the first

Ethernet packet is set to a zero.

20. (previously presented) The method of claim 17 wherein the extracting step comprises extracting an address from second, third and fourth bytes following an Ethernet type field from the first Ethernet packet.

21. (previously presented) The method of claim 17 wherein the extracting step comprises extracting an address from a lower 22 bits of second, third and fourth bytes following an Ethernet type field from the first Ethernet packet.

22. (previously presented) The method of claim 17 wherein the retrieving step comprises retrieving the security association from a memory in a security processor.

23. (previously presented) The method of claim 17 wherein the encrypting step comprises using an encryption key associated with the security association.

24. (previously presented) The method of claim 17 wherein the encrypting step comprises using an encryption algorithm defined by the security association.

25. (previously presented) The method of claim 17 wherein the extracting step comprises determining whether an Ethernet address from the first Ethernet packet matches an Ethernet address of a security processor.

26. (previously presented) A method of generating packets to be encrypted comprising the steps of:

generating a first Ethernet packet;

associating a security association with the first Ethernet packet;

identifying a memory address associated with the security association; and

generating a second Ethernet packet encapsulating the memory address and the first Ethernet packet.

27. (previously presented) The method of claim 26 wherein the generating a second Ethernet packet comprises generating an outer Ethernet header comprising an address of a security processor.

28. (previously presented) The method of claim 26 wherein the generating a second Ethernet packet comprises generating an outer Ethernet header and a manufacturer header.

29. (original) The method of claim 28 wherein the outer Ethernet header comprises an Ethernet address of a security processor.

30. (previously presented) The method of claim 28 wherein the outer Ethernet header comprises a user-specified Ethernet type field.

31. (previously presented) The method of claim 28 wherein the manufacturer header comprises the memory address.

32. (previously presented) The method of claim 28 wherein a first byte of the manufacturer header is set to zero.

33. (previously presented) The method of claim 28 wherein second, third and fourth bytes of the manufacturer header comprise the memory address.

34. (canceled)

35. (previously presented) The method of claim 26 further comprising the steps of:

receiving data to be sent over an Ethernet network; and

incorporating the data into the first Ethernet packet.

36. (previously presented) The method of claim 26 further comprising the step of transmitting the second Ethernet packet to at least one security processor.

37. (previously presented) A security processor for generating encrypted packets by processing a first Ethernet packet comprising a second Ethernet packet and a memory address associated with a security association, comprising:

a memory for storing the security association;

a Gigabit MAC for receiving the first Ethernet packet;

a processor, connected to receive at least a portion of the first Ethernet packet from the Gigabit MAC, for

extracting the memory address from the first Ethernet packet; and

retrieving the security association from the memory using the extracted memory address; and

an encryption processor, connected to the processor, for encrypting at least a portion of the second Ethernet packet according to the retrieved security association.

38. (previously presented) The security processor of claim 37 wherein the first Ethernet packet comprises an outer Ethernet header and a manufacturer header including the memory address.

39. (previously presented) The security processor of claim 37 wherein the encryption processor comprises a IPsec processor.

40. (original) The security processor of claim 37 wherein the security processor is an integrated circuit.

41-53. (canceled)